



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/843,599	04/26/2001	Bing Wang	42390P10468	8760
8791	7590	02/23/2005	EXAMINER	
BLAKELY SOKOLOFF TAYLOR & ZAFMAN 12400 WILSHIRE BOULEVARD SEVENTH FLOOR LOS ANGELES, CA 90025-1030			JACOBS, LASHONDA T	
			ART UNIT	PAPER NUMBER
			2157	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/843,599	WANG ET AL.	
	Examiner	Art Unit	
	LaShonda T Jacobs	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 01 November 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-24 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This Office Action is in response to Applicants' Amendment and Request for Reconsideration filed on November 1, 2004. Claims 1-22 are presented for further examination. Newly added claims 23-24 are presented for examination.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shi et al (hereinafter, "Shi", U.S. Pat. No. 5,875,296) in view of Wood et al (hereinafter, "Wood", U.S. Pat. No. 6,668,322).

As per claims 1, 10 and 19, Shi discloses a method, an article of manufacture and an apparatus for de-authenticating from a first web server security realm protected by an authentication scheme lacking a de-authentication operation, the method comprising:

- attempting to access a first resource in a first security realm protected by the authentication scheme (abstract and col. 8, lines 32-46);
- receiving a request for authentication credentials in response to said attempting to access the first resource (abstract and col. 8, lines 32-46); and

- supplying said authentication credentials in response to the request so as to become authenticated in the first security realm (abstract and col. 8, lines 32-46).

However, Shi does not explicitly disclose:

- accessing a logout resource in the first security realm, said logout resource configured to automatically authenticate with a second security realm on accessing thereof.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e. logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses accessing a logout resource in the first security realm, said logout resource configured to automatically authenticate with a second security realm on accessing thereof.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only

requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claims **2, 11 and 20**, Shi further discloses:

- providing a common access point executing a web browser (abstract and col. 8, lines 32-46); and
- first displaying a login web page of the second security realm so that a first user may authenticate with the first security realm and access the first resource, the login page comprising a login resource configured to perform said attempting to access the first resource (abstract and col. 8, lines 32-46);

However, Shi does not explicitly disclose:

- second displaying the login web page of the second security realm responsive to said accessing the logout resource so that a second user may authenticate with the first security realm and access the first resource.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e. logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses second displaying the login web page of the second security realm responsive to said accessing the logout resource so that a second user may authenticate with the first security realm and access the first resource.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claims 3 and 12, Shi discloses the invention substantially as claimed as discussed above.

However, Shi does not explicitly disclose:

- wherein the logout resource execute a script configured to authenticate a user with the second security realm.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e. logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses wherein the logout resource execute a script configured to authenticate a user with the second security realm.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claims 4 and 13, Shi discloses the invention substantially as claimed as discussed above.

However, Shi does not explicitly disclose:

- wherein the logout resource comprises a web page element comprising a link to the script; and
- wherein the web page element incorporates authentication credentials for the second security realm so that the user need not to provide authentication to access the second security realm.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e.

logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses wherein the logout resource comprises a web page element comprising a link to the script and wherein the web page element incorporates authentication credentials for the second security realm so that the user need not to provide authentication to access the second security realm.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claims 5 and 14, Shi discloses:

- wherein the authentication scheme comprises HTTP basic authentication (abstract, col. 1, lines 10-17, lines 61-63 and col. 3, lines 17-21).

As per claims 6, 15 and 21, Shi discloses a method, an article of manufacture and an apparatus for de-authenticating from an HTTP basic authentication comprising:

- attempting to access a first resource in a first security realm protected by HTTP basic authentication (abstract and col. 8, lines 32-46);
- responsive to said attempting to access, receiving an authentication request for controlling access to the first resource (abstract and col. 8, lines 32-46);
- supplying authentication credentials responsive to said authentication request so as to authenticate with the first security realm (abstract and col. 8, lines 32-46);

However, Shi does not explicitly disclose:

- accessing a second resource in the first security realm; and
- responsive to said accessing the second resource, automatically authenticating with a second security realm.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e. logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses accessing a second resource in the first security realm and responsive to said accessing the second resource, automatically authenticating with a second security realm.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials

and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claims **7** and **16**, Shi discloses:

- wherein said authenticating with the second security realm invalidates a prior authentication with the first security realm (col. 9, lines 11-22).

As per claims **8** and **17**, Shi further discloses:

- displaying a login element within a web browser, the login element configures to access the first resource upon activation thereof (abstract and col. 8, lines 32-46).

As per claims **9**, **18** and **22**, Shi further discloses:

- a. authenticating a first user with the first security realm (col. 9, lines 11-22);

However, Shi does not explicitly disclose:

- displaying a logout element within the web browser for performing said automatically authenticating with the second security realm; and

within a single browser session:

- b. authenticating the first user with the second security realm so as to de-authenticate the first user from the first security realm; and
- c. authenticating a second user with the first security realm.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e. logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses displaying a logout element within the web browser for performing said automatically authenticating with the second security realm, authenticating the first user with the second security realm so as to de-authenticate the first user from the first security realm and authenticating a second user with the first security realm.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claim 24, Shi discloses a de-authenticating method for a web browser, comprising:

Art Unit: 2157

- accessing a first resource in a first security realm of the web server with the web browser, the web browser automatically cache authentication credentials for a current security realm to which the web browser is authenticated (abstract and col. 8, lines 32-46);
- receiving a request for authentication responsive to requesting the first resource (abstract and col. 8, lines 32-46); and
- authenticating with the first security realm based at least in part on providing authentication credentials responsive to the request for authentication, so that the current security realm is first security realm (abstract and col. 8, lines 32-46).

However, Shi does not explicitly disclose:

- de-authenticating from the first web server security realm based at least in part on accessing a second resource of a second security realm different from the first resource of the first security realm, so that the current security realm changes fro the first security realm to the second security realm.

Wood discloses an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains for accessing one or more of enterprise applications or resources. Once authenticated in a domain, a user can later access (i.e. logout) the same or to another information resource without any additional authentication (col. 15, lines 23-26 and col. 17, lines 20-29). Therefore, Wood implicitly discloses de-authenticating from the first web server security realm based at least in part on accessing a second resource of a second security realm different from the first resource of the first security realm, so that the current security realm changes fro the first security realm to the second security realm.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wood's teaching of an access management system and method employing secure credentials in which a single sign-on is used to control access to multiple domains, for the purpose of allowing sessions credentials to be authenticated once in order to access one or more information resources without the need of further login credentials and authentication. Which would improve the security of information transactions over network [see Wood, col. 1, lines 8-10, col. 2, lines 27-30 and lines 50-55]. Thus, Shi provides the motivation to combine by utilizing a method of authentication a web client to a web server(s) as well as providing a distributed file system authentication scheme for web browsing that only requires passing of a user id and password once [see Shi col. 2, lines 38-44 and col. 3, lines 40-46].

As per claim 24, Shi discloses,

- wherein the web browser and the web server communicate using a stateless communication protocol (col. 4, lines 27-30).

Response to Arguments

3. Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat. No. 6,339,423 to Sampson et al

U.S. Pat. No. 6,601,171 to Carter et al

U.S. Pat. No. 5,649,099 to Theimer et al

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LaShonda T. Jacobs whose telephone number is 703-305-7494. The examiner can normally be reached on 8:30 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 703-308-7562. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LaShonda T. Jacobs
Examiner
Art Unit 2157

ltj
February 14, 2005


ARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Application/Control Number: 09/843,599
Art Unit: 2157

Page 14